WHAT IS CLAIMED IS:

1. A method for a client user remotely connected to a host computer by a client workstation to have securely displayed and to securely confirm that a request to perform an operation on the host computer was actually requested by the client user, the method comprising the steps of:

(1) in response to the request, generating a challenge that includes what operation to be performed on the host computer was requested, a nonce, and a query as to whether the client user made the request;

(2) encrypting the challenge;

(3) transmitting the encrypted challenge to a secure environment that contains the client user's private key;

(4) decrypting the challenge in the secure environment and securely displaying the decrypted challenge;

(5) waiting for confirmation from the client user that securely confirms either that the client user did or did not make the request to perform the operation on the host computer;

(6) if the client user confirms that:

(a) the client user did not make the request, transmitting a reply encrypted with the host computer's public key to the host computer that contains a negative response and the nonce; or

(b) client user did make the request, transmitting a reply encrypted with the host computer's public key to the host computer that contains a positive response and the nonce.

2. The method of claim 1 wherein the request is for access to a resource on the host computer.

3. The method of claim 2 wherein the challenge encrypted during step (2) is encrypted with the client user's public key.

4. The method of claim 2 wherein the secure environment includes an intelligent security token containing the client user's private key that is capable of decrypting the encrypted challenge during step (4).

5. The method of claim 4 wherein the intelligent security token is a smart card and wherein the secure environment includes a smart card reader associated with the smart card and in communication with the client workstation, a secure display unit that is not directly accessible to or modifiable from the client workstation and that is capable of displaying the decrypted challenge during step (4), and a secure input device that is not directly accessible to or modifiable from the client workstation and that is capable of performing step (6).

6. The method of claim 5 wherein the display unit displays during step (4) the resource that was requested and the operation that was to be performed with the resource.

7. The method of claim 5 wherein the client workstation is the client's personal computer and wherein the client computer has residing thereon client computer software that is capable of passing the encrypted challenge during step (3) without modification to the reader and passing the encrypted reply to the host computer during step (6) without modification.

8. The method of claim 2 wherein the client user is prompted during step (5) to confirm that the client user did or did not request access to the resource on the host computer.

9. The method of claim 2 which further comprises the step of decrypting the reply transmitted during step (6) and:

(a) if the decrypted reply contains a negative response, deny the request to perform the operation on the host computer; or

(b) if the decrypted reply contains a positive response, pass through the request to perform the operation on the host computer to an authorization system of the host computer.

10. A system for securely displaying and securely confirming that a request to access a resource on a server computer was actually requested by the client user, the system comprising:

(a) a server computer having at least one resource;

(b) server computer software residing on the server computer that is capable of generating an encrypted challenge to a request for the at least one resource that includes what the at least one resource requested was, a nonce, and a query as to whether the client user made the request, and that is capable of decrypting an encrypted reply transmitted from the secure environment;

(c) a client computer in communication with the server computer;

(d) client computer software residing on the client computer that is capable of passing an encrypted challenge to the secure environment without modification and passing an encrypted reply from the secure environment without modification to the server computer;

(e) a secure environment that includes:

(1) a smart card reader in communication with the client computer;

(2) a smart card that is capable of communicating with the reader and that contains the client user's private key;

(3) reader computer software residing on the reader that is capable, in association with the smart card, of decrypting an encrypted challenge, transmitting the decrypted challenge to a secure display unit, receiving a reply from a secure input device, encrypting the reply received from the input device and transmitting the encrypted reply to the client computer;

(4) a secure display unit capable of securely displaying a decrypted challenge from the reader such that an intruder or

computer virus potentially having access to the client computer cannot modify what is displayed;

(5) a secure input device associated with the reader that is capable of responding to a reply from the client user as to whether or not the request for access to the at least one resource was actually requested by the client user and is configured such that an intruder or computer virus potentially having access to the client computer cannot modify input received by the input device.

11. The system of claim 10 wherein the server computer software residing on the server computer uses the client user's public key as an encryption key for the generating the encrypted challenge.

12. The system of claim 10 wherein the display unit is capable of displaying the resource that was requested and the operation that was to be performed with the resource.

13. The system of claim 10 wherein the smart card is capable of being inserted into the reader.

14. The system of claim 13 wherein the input device is connected to the reader.

15. The system of claim 13 wherein the client user is prompted by the secure environment to confirm that the client user did or did not request access to the resource on the server computer.

16. Software for use in a system for securely displaying and securely confirming that a request to perform an operation on a server computer was actually requested by the client user, the system including a server computer, a client computer in communication with the server computer, and a secure environment that has a smart card reader in communication with the client computer, a smart card that is capable

of communicating with the reader and that contains the client user's private key, a secure display unit capable of securely displaying a decrypted challenge from the reader such that an intruder or computer virus potentially having access to the client computer cannot modify what is displayed and a secure input device associated with the reader that is capable of responding to a reply from the client user as to whether or not the request to perform the operation was actually requested by the client user and is configured such that an intruder or computer virus potentially having access to the client computer cannot modify input received by the input device, the software comprising:

(a) a server computer software component that can reside on the server computer and is capable of generating an encrypted challenge to a request to perform the operation that includes what operation to be performed on the server computer was requested, a nonce, and a query as to whether the client user made the request , and that is capable of decrypting an encrypted reply transmitted from the secure environment;

(b) a client computer software component that can reside on the client computer and is capable of passing an encrypted challenge to the secure environment without modification and passing an encrypted reply from the secure environment without modification to the server computer; and

(c) a computer software component that can reside on the reader or the smart card, and that is capable, in association with the smart card, of decrypting an encrypted challenge, transmitting the decrypted challenge to a secure display unit, receiving a reply from the secure input device, encrypting the reply received from the input device and transmitting the encrypted reply to the client computer.

17. The software of claim 16 that is stored and installable from one or more nonvolatile electronic storage media.

18. The software of claim 17 wherein the electronic media are floppy disks or CD ROM disks.

19. The software of claim 16 which has instructions provided or associated therewith for how to use the software with the system, how to install the software on the system, or how to use with and install the software on the system.

20. The software of claim 16 wherein the computer software component (c) is a reader software component that is capable of residing on the reader.